



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/994,919	11/28/2001	Winston Donald Keech	46354.010500	7412
22191	7590	10/18/2005	EXAMINER	
GREENBERG-TRAURIG 1750 TYSONS BOULEVARD, 12TH FLOOR MCLEAN, VA 22102			DOAN, TRANG T	
			ART UNIT	PAPER NUMBER

2131

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/994,919	Applicant(s) KEECH, WINSTON DONALD	
	Examiner Trang Doan	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 7/22/2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 3/01/2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>07/22/2004</u> . | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2131

Claims 1-27 have been examined.

Priority

The application is filed on 11/28/2001 but claims the benefit of foreign priority has been made and acknowledged.

Therefore, the effective filing date for the subject matter defined in the pending claims in this application is 11/28/2000 on the benefit of foreign priority date.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 7 and 23 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
3. Claim s 7 and 23 recite the limitation "different" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 10, 12, 17 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak et al. U.S. Patent 6289450 (hereinafter Pensak) in view of Marvit et al. U.S Patent 6625734 (hereinafter Marvit).

Regarding to claim 1, Pensak teaches a method of transferring a data file having a file name from a first computer operated by a first user to a second computer operated by a second user, under control of a third computer, comprising the steps of:

i) in the first computer, the first user selecting a data file for transfer and establishing a communications link with the third computer (Pensak: column 5 lines 27-38);

ii) verifying an identity of the first user to the third computer by way of verification communications between the first and third computers (Pensak: column 8 lines 30-34);

iv) transmitting the file name of the data file from the first computer to the third computer, together with first user identification information and the unique key code (Pensak: column 2 lines 46-52 and column 8 lines 30-34);

vi) verifying an identity of the second user to the third computer by way of verification communications between the second and third computers (Pensak: column 8 lines 7-46);

vii) upon successful verification of the identity of the second user, transmitting the file name of the data file from the second computer to the third computer with a request for the unique key code (Pensak: column 8 lines 19-34); and

viii) transmitting the unique key code from the third computer to the second computer so as to cause the executable file to unwrap or decrypt the data file and to

Art Unit: 2131

allow access thereto in the second computer by the second user (Pensak: column 8 lines 34-46).

Pensak does not teach:

iii) in the first computer, wrapping or encrypting the data file within an executable file adapted to unwrap or decrypt the data file only upon activation by a unique key code, and then transmitting the executable file containing the wrapped or encrypted data file directly to the second computer together with first user identification information and the file name of the data file;

v) in the second computer, upon receipt of the executable file containing the wrapped or encrypted data file and upon attempted access thereto by the second user, establishing a communications link with the third computer;

However, Marvit teaches:

iii) in the first computer, wrapping or encrypting the data file within an executable file adapted to unwrap or decrypt the data file only upon activation by a unique key code, and then transmitting the executable file containing the wrapped or encrypted data file directly to the second computer together with first user identification information and the file name of the data file (Marvit: column 5 lines 35-56 and column 7 lines 35-39);

v) in the second computer, upon receipt of the executable file containing the wrapped or encrypted data file and upon attempted access thereto by the second user, establishing a communications link with the third computer (Marvit: column 5 lines 57-65);

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Marvit into Pensak's invention providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information (Pensak: column 1 lines 16-21). The ordinary skilled person would have been motivated to make modification to Pensak because there is a need to control and track access to information disseminated on communications networks. There is a particular need for a comprehensive approach for controlling and tracking access to data disseminated on communications networks (Marvit: column 2 lines 1-5).

Regarding to claim 10, the rejection of claim 1 is incorporated and further Pensak does not explicitly teach wherein the third computer maintains a record of transactions between the first, second and third computers so as to permit an audit trail to be established.

However, Marvit teaches wherein the third computer maintains a record of transactions between the first, second and third computers so as to permit an audit trail to be established (Marvit: column 3 lines 11-56).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Marvit into Pensak's invention providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information (Pensak: column 1 lines 16-21). The ordinary skilled person would have been motivated to make modification to Pensak because there is a need to control and track access to

Art Unit: 2131

information disseminated on communications networks. There is a particular need for a comprehensive approach for controlling and tracking access to data disseminated on communications networks (Marvit: column 2 lines 1-5).

Regarding to claim 12, Pensak teaches a method of transferring a data file to a first computer from a second computer, the method comprising the steps of:

i) establishing a communications link between the first and second computers (Pensak: column 4 lines 10-19);

ii) selecting, by way of the first computer, a data file for transfer from the second computer (Pensak: column 5 lines 46-56);

iii) in the second computer, wrapping or encrypting the data file within an executable file adapted to unwrap or decrypt the data file only upon activation by a unique key code, and then transmitting the executable file containing the wrapped or encrypted data file to the first computer (Pensak: column 5 lines 46-56);

Pensak does not teach:

iv) verifying an identity of a user of the first computer to the second computer by way of verification communications between the first and second computers;

v) upon successful verification of the user of the first computer, transmitting the unique key code to the first computer.

However, Marvit teaches:

iv) verifying an identity of a user of the first computer to the second computer by way of verification communications between the first and second computers (Pensak: column 8 lines 7-46);

v) upon successful verification of the user of the first computer, transmitting the unique key code to the first computer (Pensak: column 8 lines 34-46).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Marvit into Pensak's invention providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information (Pensak: column 1 lines 16-21). The ordinary skilled person would have been motivated to make modification to Pensak because there is a need to control and track access to information disseminated on communications networks. There is a particular need for a comprehensive approach for controlling and tracking access to data disseminated on communications networks (Marvit: column 2 lines 1-5).

Regarding to claim 17, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding to claim 26, the rejection of claim 17 is incorporated and further this claim has limitation that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

6. Claims 2-7, 11, 13, 18-23 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak in view of Marvit, and further in view of Bostley, III et al. U.S. Patent 6201871 (hereinafter Bostley).

Regarding to claim 2, the rejection of claim 1 is incorporated and further Pensak and Marvit do not explicitly teach wherein the identity of the first user is verified in step ii) above by way of the first user applying a first user mask code to a pseudo-random

Art Unit: 2131

security string in the first computer so as to generate a first user volatile identification code, the first user transmitting the first user volatile identification code to the third computer and the third computer comparing the first user volatile identification code with a first check volatile identification code obtained by applying the first user mask code to the pseudo-random string in the third computer, identity verification taking place when the first user volatile identification code and the first check volatile identification codes are found to match each other.

However, Bostley teaches wherein the identity of the first user is verified in step ii) above by way of the first user applying a first user mask code to a pseudo-random security string in the first computer so as to generate a first user volatile identification code, the first user transmitting the first user volatile identification code to the third computer and the third computer comparing the first user volatile identification code with a first check volatile identification code obtained by applying the first user mask code to the pseudo-random string in the third computer, identity verification taking place when the first user volatile identification code and the first check volatile identification codes are found to match each other (Bostley: column 5 lines 34-49).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Bostley into the combination Pensak and Marvit's invention providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information (Pensak: column 1 lines 16-21). The ordinary skilled person would have been motivated to make modification to Pensak and Marvit because the wireless

communication system would be greatly improved by a technology that improves the security of A-Keys in a wireless communications system (Bostley: column 2 lines 1-5).

Regarding to claim 3, the rejection of claim 1 is incorporated and further Pensak and Marvit do not explicitly teach wherein the identity of the second user is verified in step vi) above by way of the second user applying a second user mask code to a pseudo-random security string in the second computer so as to generate a second user volatile identification code, the second user transmitting the second user volatile identification code to the third computer and the third computer comparing the second user volatile identification code with a second check volatile identification code obtained by applying the second user mask code to the pseudo-random string in the third computer, identity verification taking place when the second user volatile identification code and the second check volatile identification codes are found to match each other.

However, Bostley teaches wherein the identity of the second user is verified in step vi) above by way of the second user applying a second user mask code to a pseudo-random security string in the second computer so as to generate a second user volatile identification code, the second user transmitting the second user volatile identification code to the third computer and the third computer comparing the second user volatile identification code with a second check volatile identification code obtained by applying the second user mask code to the pseudo-random string in the third computer, identity verification taking place when the second user volatile identification code and the second check volatile identification codes are found to match each other (Bostley: column 5 lines 34-49).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Bostley into the combination of Pensak and Marvit's invention providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information (Pensak: column 1 lines 16-21). The ordinary skilled person would have been motivated to make modification to Pensak and Marvit because the wireless communication system would be greatly improved by a technology that improves the security of A-Keys in a wireless communications system (Bostley: column 2 lines 1-5).

Regarding to claim 4, the rejection of claim 3 is incorporated and further Pensak and Marvit do not explicitly teach wherein the first user mask code and the second user mask code are applied to the same pseudo-random security string.

However, Bostley teaches wherein the first user mask code and the second user mask code are applied to the same pseudo-random security string (Bostley: column 5 lines 35-65).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Bostley into the combination of Pensak and Marvit's invention providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information (Pensak: column 1 lines 16-21). The ordinary skilled person would have been motivated to make modification to Pensak and Marvit because the wireless communication system would be greatly improved by a technology that improves the security of A-Keys in a wireless communications system (Bostley: column 2 lines 1-5).

Regarding to claim 5, the rejection of claim 4 is incorporated and further Pensak and Marvit do not explicitly teach wherein the pseudo-random string is generated by the third computer and transmitted firstly to the first computer and then from the first computer to the second computer.

However, Bostley teaches wherein the pseudo-random string is generated by the third computer and transmitted firstly to the first computer and then from the first computer to the second computer (Bostley: column 5 lines 35-65).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Bostley into the combination of Pensak and Marvit's invention providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information (Pensak: column 1 lines 16-21). The ordinary skilled person would have been motivated to make modification to Pensak and Marvit because the wireless communication system would be greatly improved by a technology that improves the security of A-Keys in a wireless communications system (Bostley: column 2 lines 1-5).

Regarding to claim 6, the rejection of claim 4 is incorporated and further Pensak and Marvit do not explicitly teach wherein the pseudo-random string is generated by the third computer and transmitted firstly to the first computer and then from the third computer to the second computer.

However, Bostley teaches wherein the pseudo-random string is generated by the third computer and transmitted firstly to the first computer and then from the third computer to the second computer (Bostley: column 5 lines 35-65).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Bostley into the combination of Pensak and Marvit's invention providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information (Pensak: column 1 lines 16-21). The ordinary skilled person would have been motivated to make modification to Pensak and Marvit because the wireless communication system would be greatly improved by a technology that improves the security of A-Keys in a wireless communications system (Bostley: column 2 lines 1-5).

Regarding to claim 7, the rejection of claim 3 is incorporated and further Pensak and Marvit do not explicitly teach wherein the first user mask code and the second user mask code are applied to different pseudo-random security strings.

However, Bostley teaches wherein wherein the first user mask code and the second user mask code are applied to different pseudo-random security strings (Bostley: column 5 lines 35-65).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Bostley into the combination of Pensak and Marvit's invention providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information (Pensak: column 1 lines 16-21). The ordinary skilled person would have been motivated to make modification to Pensak and Marvit because the wireless communication system would be greatly improved by a technology that improves the security of A-Keys in a wireless communications system (Bostley: column 2 lines 1-5).

Regarding to claim 11, the rejection of claim 2 is incorporated and further Pensak, Marvit and Bostley teach wherein the first and/or second user volatile identification codes are stored as digital signatures in the third computer in combination with the associated pseudo-random security string (Pensak: column 17 lines 42-59).

Regarding to claim 13, the rejection of claim 12 is incorporated and further this claim has limitation that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

Regarding to claim 18, the rejection of claim 17 is incorporated and further this claim has limitation that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

Regarding to claim 19, the rejection of claim 18 is incorporated and further this claim has limitation that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

Regarding to claim 20, the rejection of claim 19 is incorporated and further this claim has limitation that is similar to those of claim 4, thus it is rejected with the same rationale applied against claim 4 above.

Regarding to claim 21, the rejection of claim 20 is incorporated and further this claim has limitation that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

Regarding to claim 22, the rejection of claim 20 is incorporated and further this claim has limitation that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

Regarding to claim 23, the rejection of claim 19 is incorporated and further this claim has limitation that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

Regarding to claim 27, the rejection of claim 18 is incorporated and further this claim has limitation that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

7. Claims 8, 14 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak in view of Marvit, and further in view of Wilfong U.S. Patent 5754652 (hereinafter Wilfong).

Regarding to claim 8, the rejection of claim 1 is incorporated and further Pensak and Marvit do not explicitly teach:

i) said secure user code entry interface contains at least one active display for entry of at least one digit of said user mask code by the user; wherein said active display illuminates or highlights at least one display digit within said active display and said user enters said at least one digit of said user mask code by a response through an input device at a response time when said at least one display digit which corresponds with said at least one digit of said user mask code is illuminated or highlighted in said active display; and

ii) a random run on time is added to said response time to extend said at least one active display.

However, Wilfong teaches i) said secure user code entry interface contains at least one active display for entry of at least one digit of said user mask code by the

Art Unit: 2131

user; wherein said active display illuminates or highlights at least one display digit within said active display and said user enters said at least one digit of said user mask code by a response through an input device at a response time when said at least one display digit which corresponds with said at least one digit of said user mask code is illuminated or highlighted in said active display (Wilfong: column 2 lines 28-41); and ii) a random run on time is added to said response time to extend said at least one active display (Wilfong: column 2 lines 28-41).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Wilfong into the combination of Pensak and Marvit's invention providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information (Pensak: column 1 lines 16-21). The ordinary skilled person would have been motivated to make modification to Marvit because to provide for securely entering a PIN number in a public location.

Regarding to claim 14, the rejection of claim 12 is incorporated and further this claim has limitations that is similar to those of claim 8, thus it is rejected with the same rationale applied against claim 8 above.

Regarding to claim 24, the rejection of claim 17 is incorporated and further this claim has limitations that is similar to those of claim 8, thus it is rejected with the same rationale applied against claim 8 above.

8. Claims 9, 15 and 25 are is rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak in view of Marvit, and further in view of Bostley, and further in view of Girolomo Cardano (hereinafter Grilles).

Regarding to claim 9, the rejection of claim 2 is incorporated and further Pensak, Marvit, and Bostley do not explicitly teach:

- i) the pseudo-random string comprises a first linear array of characters, each character having a given numerical position in the first array (first, second, third etc.);
- ii) the mask code comprises a second linear array of numbers, each number having a given numerical position in the second array (first, second, third etc.); and
- iii) the volatile identification code is generated by applying the mask code to the pseudo-random string so as sequentially to select numerical positions in the first array on the basis of the numbers in the second array, taken in positional order, and to return the characters thereby selected from the first array in sequence so as to form a third linear array, this third linear array forming the volatile identification code.

However, Grilles teaches:

- i) the pseudo-random string comprises a first linear array of characters, each character having a given numerical position in the first array (first, second, third etc.) (Grilles: "Cardano Grilles" pages 1-3);
- ii) the mask code comprises a second linear array of numbers, each number having a given numerical position in the second array (first, second, third etc.) (Grilles: "Cardano Grilles" pages 1-3); and

iii) the volatile identification code is generated by applying the mask code to the pseudo-random string so as sequentially to select numerical positions in the first array on the basis of the numbers in the second array, taken in positional order, and to return the characters thereby selected from the first array in sequence so as to form a third linear array, this third linear array forming the volatile identification code (Grilles: "Cardano Grilles" pages 1-3).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Grilles into the combination of Pensak, Marvit and Bostley's invention providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information (Pensak: column 1 lines 16-21). The ordinary skilled person would have been motivated to make modification to Pensak, Marvit and Bostley because to implement Grilles' message masking method to pass a message secretly from one party to second without being compromised by a third party.

Regarding to claim 15, the rejection of claim 13 is incorporated and further this claim has limitation that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

Regarding to claim 25, the rejection of claim 18 is incorporated and further this claim has limitation that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

9. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Goldfine et al. U.S. Patent 5343529 (hereinafter Goldfine) in view of Marvit.

Regarding to claim 16, Goldfine teaches a method of transferring a data file to a first computer having a first telecommunications address from a second computer having a second telecommunications address, comprising the steps of:

i) transmitting a request for the data file from the first computer to the second computer, the request including data identifying the data file and the first telecommunications address (Goldfine: column6 lines 29-55);

iii) assigning a unique identification string to the executable file in the second computer, the unique identification string being further associated in the second computer with the first telecommunications address (Goldfine: column 6 lines 42-50);

iv) transmitting the executable file (containing the data file) and the unique identification string from the second computer to the first computer (Goldfine: column 4 lines 25-44);

v) causing a message to be displayed by the first computer showing the unique identification string and requesting a user to call a predetermined telephone number from a telephone operated by the user (Goldfine: column 4 lines 25-44);

vi) receiving a telephone call from the telephone operated by the user, determining its telephone number and receiving the unique identification string from the user (Goldfine: column 4 lines 25-44);

vii) in the second computer, generating a pseudo-random string, associating the pseudo-random string with the unique identification string and the telephone number of the telephone operated by the user, and transmitting the pseudo-random string to the

Art Unit: 2131

telephone operated by the user (Goldfine: column 6 lines 45-50 and column 4 lines 34-44);

viii) applying a mask code, known to the user and to the second computer, to the pseudo-random identification string so as to generate a volatile identification code in accordance with predetermined rules (Goldfine: column 4 lines 40-68);

ix) transmitting the volatile identification code to the second computer, either from the telephone operated by the user in which case the volatile identification code is transmitted together with the telephone number of the telephone operated by the user, or from the first computer in which case the volatile identification code is transmitted together with the first telecommunications address, the telephone number or the first telecommunications address respectively serving to identify the first computer, the user and the executable file (Goldfine: column 4 lines 40-53);

x) in the second computer, checking that the volatile identification code matches a volatile identification code generated therein by applying the mask code to the pseudo-random string and (Goldfine: column 4 lines 45-53), if so;

However, Goldfine does not teach in the second computer, wrapping or encrypting the data file within an executable file adapted to unwrap or decrypt the data file only upon activation by a unique key; transmitting the key code to the first computer so as to enable the executable file to unwrap or decrypt the data file and to install this on the first computer.

Marvit teaches in the second computer, wrapping or encrypting the data file within an executable file adapted to unwrap or decrypt the data file only upon activation

Art Unit: 2131

by a unique key code (Marvit: column 5 lines 35-56 and column 7 lines 35-39); transmitting the key code to the first computer so as to enable the executable file to unwrap or decrypt the data file and to install this on the first computer (Marvit: column 5 lines 57-68 and column 6 lines 1-6).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Marvit into Goldfine's invention to prevent theft of communication services (Goldfine: column 1 lines 19-20). The ordinary skilled person would have been motivated to make modification to Goldfine because there is a need to control and track access to information disseminated on communications networks. There is a particular need for a comprehensive approach for controlling and tracking access to data disseminated on communications networks (Marvit: column 2 lines 1-5).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Trang Doan whose telephone number is (571) 272-0740. The examiner can normally be reached on Monday-Friday.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Trang Doan
Examiner
Art Unit 2131

T.D.
September 26, 2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100